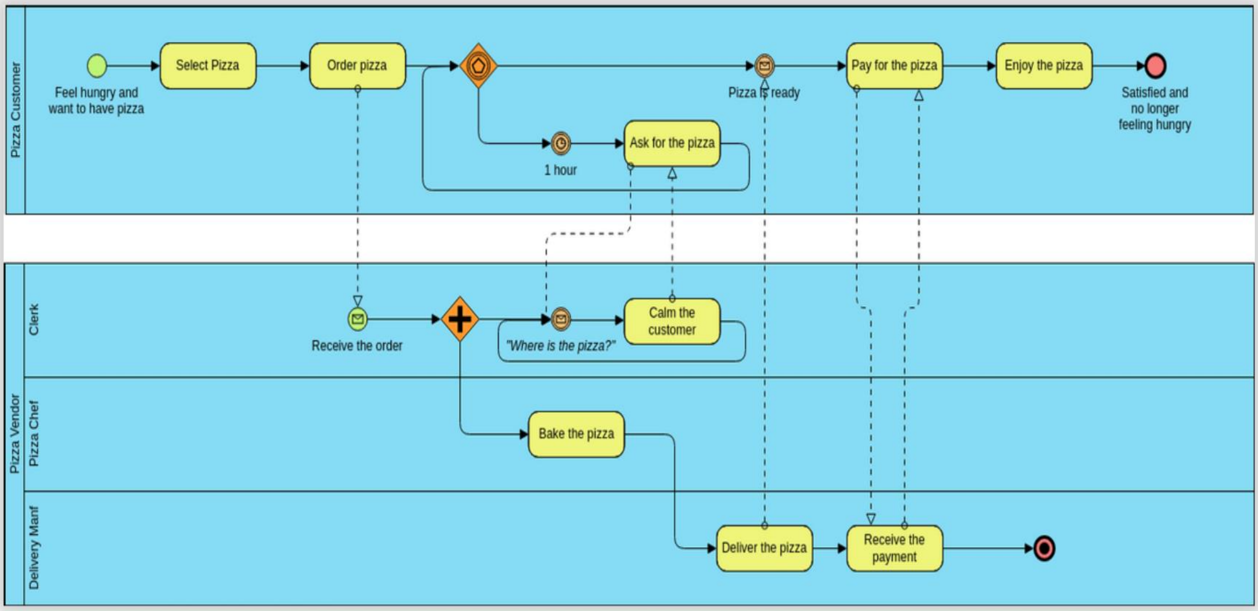
Risk Analysis of PIZZERIA



BPMN: PIZZERIA

DESCRIPTION

The BPMN (Business Process Model and Notation) diagram outlines the processes involved in the operations of a pizzeria, detailing the interactions between different roles within the organization, including the customer, clerk, pizza chef, and delivery personnel.

- Swimlanes and Roles:
  a. Pizza Customer: This swimlane represents the activities performed by the customer.
  b. Clerk: This swimlane represents the activities performed by the clerk handling orders.
  c. Pizza Vendor: Includes activities of both the clerk and pizza chef.
  d. Delivery Person: Represents the activities performed by the delivery personnel.

- Processes:

1. Customer Process:
    a. Feel Hungry and Want to Have Pizza: The process starts when a customer feels hungry and decides to order a pizza.
    b. Select Pizza: The customer selects the type of pizza they want.
    c. Order Pizza: The customer places an order for the selected pizza.
    d. Ask for the Pizza (After 1 Hour): If the pizza is not delivered within an hour, the customer inquiries about the status of their order.
    e. Pay for the Pizza: Once the pizza is delivered, the customer pays for it.
    f. Enjoy the Pizza: The customer consumes the pizza.
    g. Satisfied and No Longer Feeling Hungry: The process ends with the customer being satisfied.
2. Clerk Process:
    a. Receive the Order: The clerk receives the pizza order from the customer.
    b. Calm the Customer: If the customer inquiries about the pizza due to a delay, the clerk addresses the customer's concerns.
3. Pizza Chef Process:
    a. Bake the Pizza: The pizza chef prepares and bakes the pizza once the order is received.
4. Delivery Personnel Process:
    a. Deliver the Pizza: The delivery personnel are responsible for delivering the pizza to the customer.
    b. Receive the Payment: The delivery personnel collect the payment from the customer.
5. Interactions and Workflow:
    a. Order Placement: The customer places an order, which is received by the clerk.
    b. Order Processing: The clerk communicates the order to the pizza chef, who then bakes the pizza.

    c. Delivery: The baked pizza is handed over to the delivery personnel, who deliver it to the customer.
    d. Customer Inquiry: If the delivery is delayed, the customer inquiries about the order, and the clerk addresses the concern.
    e. Completion: Upon delivery, the customer pays for the pizza and enjoys the meal, completing the process.

6. Events and Gateways:
    a. Timer Event (1 Hour): This indicates that an hour has passed since the order was placed.
    b. Message Events: Indicate communication points such as receiving the order, pizza ready notification, and customer inquiries.
    c. Parallel Gateway: Indicates that multiple activities (baking the pizza and handling customer inquiries) can occur simultaneously.

Phase 0: Scope and Delimitations

PIZZERIA relies heavily on Information Technology (IT) systems to manages its operations effectively.
Here the key IT components that would be present in this company:

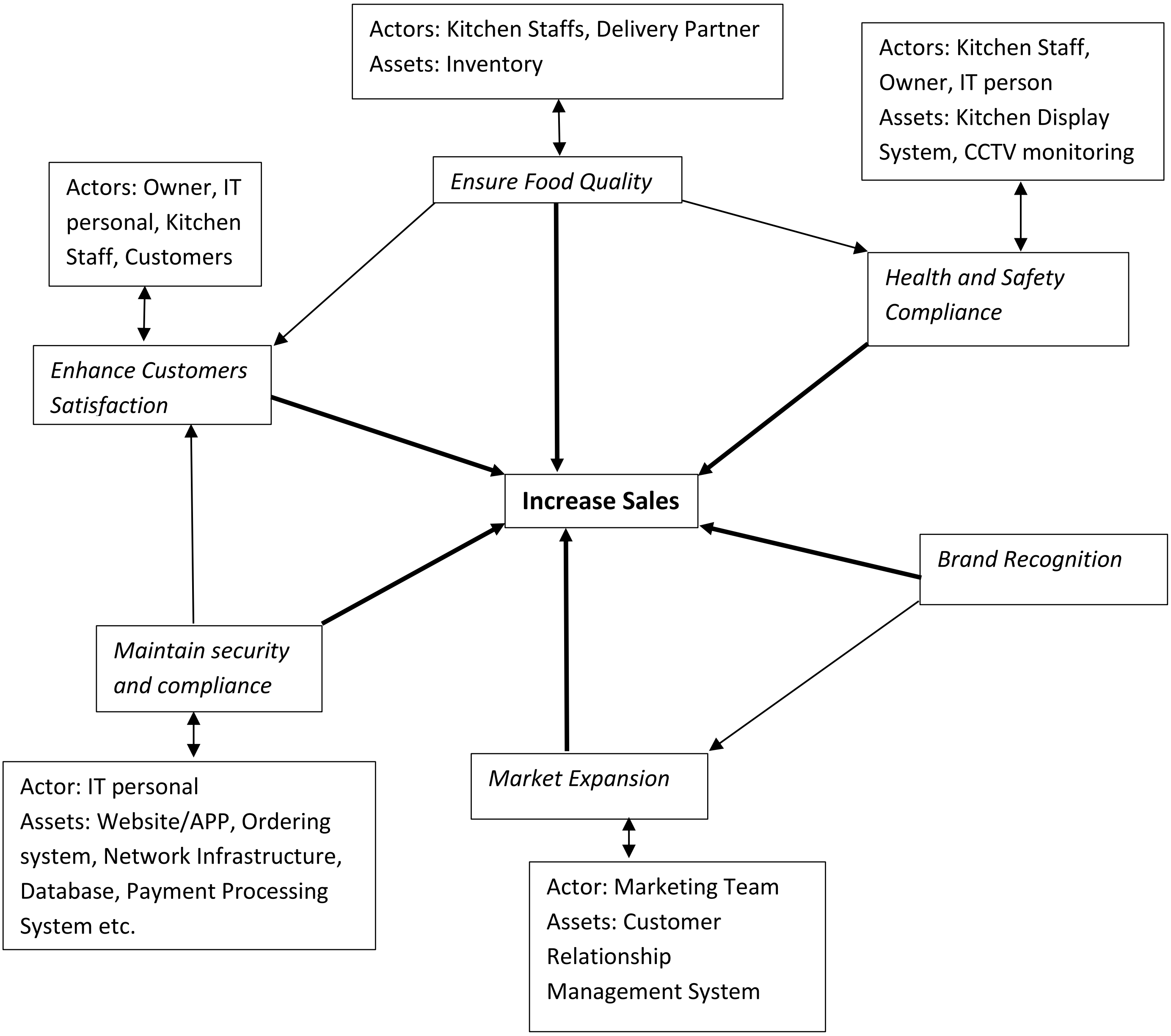
- Mobile application or Website.
- Geolocation and mapping system. (Tracking Delivery partners)
- User Authentication and Registration.
- Network Infrastructure.
- Security camera and surveillance system. (Security cameras are installed to monitor the premises for safety and security.)
- Point of Sale System. (This is used for processing orders, managing inventory, and handling payments. It may consist of hardware such as terminals and printers, as well as software for managing transactions.)
- Kitchen Display system. (to display orders in the kitchen for food preparation. It helps streamline the cooking process and ensures orders are prepared efficiently.)
- Inventory Management System. (This system tracks ingredients, supplies, and stock levels to ensure that the pizzeria has enough inventory to meet demand. It helps optimize purchasing and minimize waste.)
- Ordering System. (This includes both in-store and online ordering systems where customers can place orders for delivery, takeout, or dine-in. It may involve mobile apps, websites
- Payment processing System. (securely processes credit card transactions and other forms of payment. It must comply with Payment Card Industry Data Security Standard (PCI DSS) requirements to protect sensitive cardholder data.)
- Customers Relationship management system. (manages customer data, including contact information, order history,

and preferences. It can be used for marketing, loyalty programs, and personalized customer experiences.)

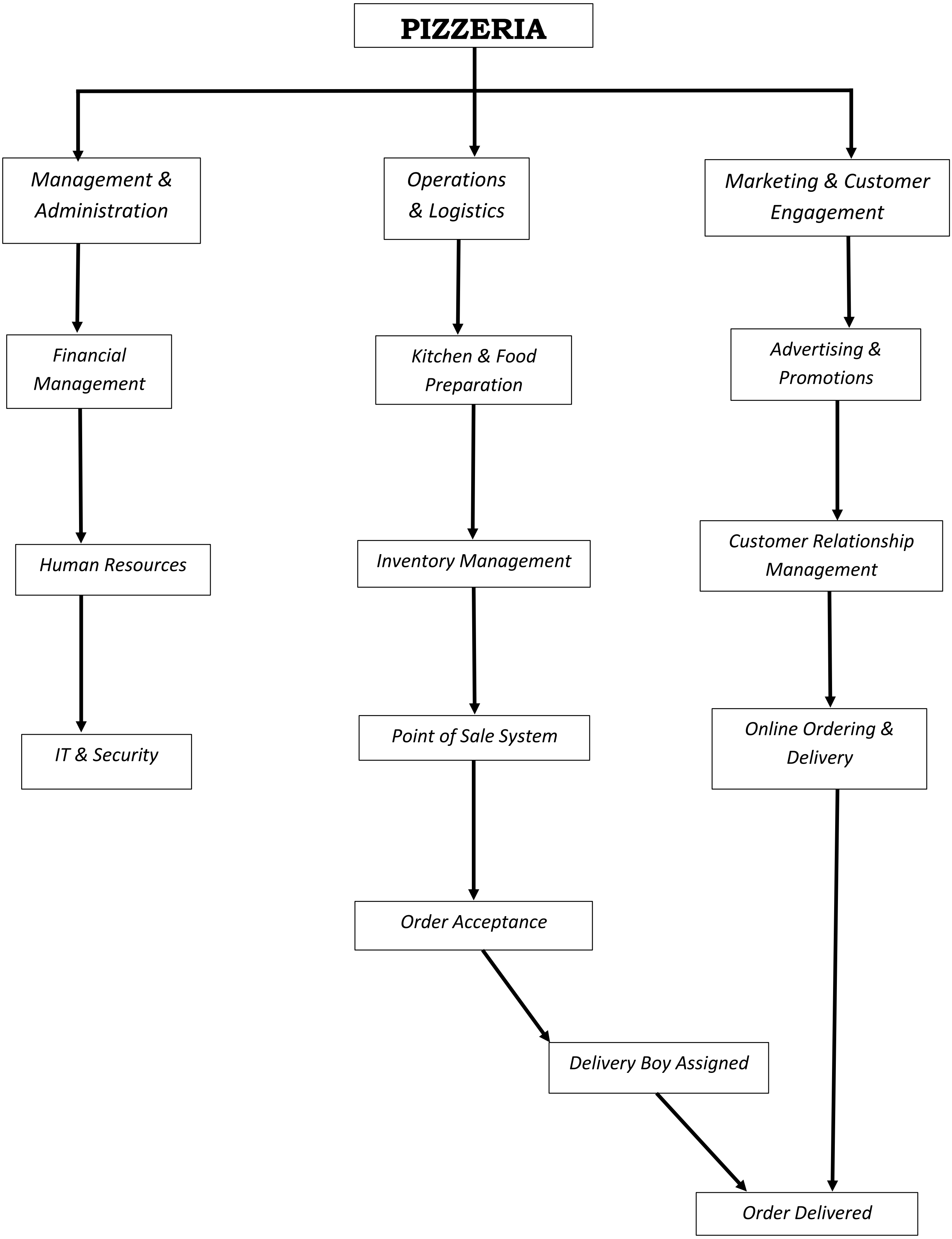
- Database management. (backing up and storing critical data, such as transaction records, customer information, and menu items. Regular backups are essential for data protection and disaster recovery.)

Phase 1: Business value of System

- **Business Goal:**


Actors: Kitchen Staffs, Delivery Partner
Assets: Inventory
Actors: Kitchen Staff, Owner, IT person
Assets: Kitchen Display System, CCTV monitoring
Actors: Owner, IT personal, Kitchen Staff, Customers
Ensure Food Quality
Health and Safety Compliance
Enhance Customers Satisfaction
Increase Sales
Brand Recognition
Maintain security and compliance
Market Expansion
Actor: IT personal
Assets: Website/APP, Ordering system, Network Infrastructure, Database, Payment Processing System etc.
Actor: Marketing Team
Assets: Customer Relationship Management System

- **Business Architecture:**



- **Negative Business Impact:**

Category	Impact	Directly Affected
Financial Loss	*Direct Costs:* Costs related to breach management (cybersecurity experts, forensic investigations, legal fees).	Finance, IT
	Fines and Penalties: Regulatory fines due to non-compliance with data protection laws (GDPR, HIPAA, PCI DSS).	Finance, Legal
	Revenue Loss: Loss of sales and business opportunities due to system downtime or loss of customer trust.	Finance, Sales
Reputational Damage	*Customer Trust:* Erosion of trust and confidence in the business's ability to protect data, leading to customer attrition.	Customers, Marketing
	Brand Image: Negative media coverage and public perception, damaging the brand’s reputation and making it harder to attract new customers.	Marketing, PR
	Competitive Disadvantage: Competitors capitalizing on the breach to attract disillusioned customers.	Sales, Marketing
Operational Damage	*System Downtime:* Interruption of business operations, leading to delays in order processing, inventory management, and other critical functions.	Operations, IT, Delivery Staff
	Resource Allocation: Diverting resources to manage the breach, affecting ongoing projects and business development activities.	All Department
Legal and Regulatory	*Litigation:* Legal actions from affected customers, partners, or shareholders, resulting in costly settlements or judgments.	Legal, Finance
	Regulatory Scrutiny: Increased scrutiny and audits from regulatory bodies, leading to further compliance costs and operational constraints.	Compliance, Legal, Operations
Customer Impact	*Data Loss:* Compromise of customer data, leading to identity theft or fraud.	Customers

	Service Interruption: Inability to provide services during the breach, causing customer inconvenience and dissatisfaction.	Customers, Operations
Employee Impact	*Morale and Productivity:* Decreased employee morale and productivity due to uncertainty and increased workload related to managing the breach.	Employee, HR
	Job Security: Potential layoffs or restructuring as a result of financial losses and reputational damage.	Employee, HR
Long-Term Strategic Impact	*Investment and Growth:* Difficulty attracting investors or securing funding due to perceived higher risks, affecting long-term growth and expansion plans.	Management, Investors
	Market Position: Loss of market position and competitive edge, making it harder to regain market share.	Management, Sales, Marketing

Phase 2: System Definition and Decomposition

For Phase 2 of a risk analysis for a pizzeria, we'll identify the ICT (Information and Communications Technology) system components that are critical to the business operations. This includes hardware, software, network infrastructure, data stores, and external interfaces. Here’s a detailed breakdown:

ICT System Components for Pizzeria

Hardware Components

- Servers:

Application Server

Database Server

Web Server

Backup Server

- Workstations:

  Employee Workstations

  POS Terminals

- Network Devices:

  Routers

  Switches

  Firewall

  Wi-Fi Access Points

Software Components

- Operating Systems:

  Server OS: Linux/Windows Server for servers.

  Workstation OS: Windows, macOS, or Linux for employee workstations and POS terminals.

- Applications:

  Order Processing System: Manages customer orders, updates order status, and communicates with the kitchen display system.

  Inventory Management System: Tracks stock levels, manages supplier orders, and updates inventory data.

  Customer Relationship Management (CRM) System: Manages customer data, marketing campaigns, and loyalty programs.

  Financial Management Software: Manages financial transactions, accounting, and generates financial reports.

  Web Application: Allows customers to place orders online and interacts with the order processing system.

- Security Software:

  Antivirus/Anti-malware: Protects servers and workstations from malicious software.

  Intrusion Detection System (IDS)/Intrusion Prevention System (IPS): Monitors network traffic for suspicious activity.

  Encryption Software: Encrypts sensitive data at rest and in transit.

Network Infrastructure

- Local Area Network (LAN):

  Internal Network: Connects servers, workstations, and other network devices within the pizzeria.

  Guest Network: A separate network for customers' Wi-Fi access, isolated from the internal network.

- Wide Area Network (WAN):

  Internet Connection: Provides external connectivity for online orders, supplier communications, and remote management.

Data Stores

- Databases:

  Customer Database: Stores customer information, order history, and loyalty program details.

  Inventory Database: Stores information on stock levels, supplier details, and order history.

  Order Database: Keeps records of all orders placed, both online and in-store.

  Financial Database: Contains financial transaction data, accounting records, and financial reports.

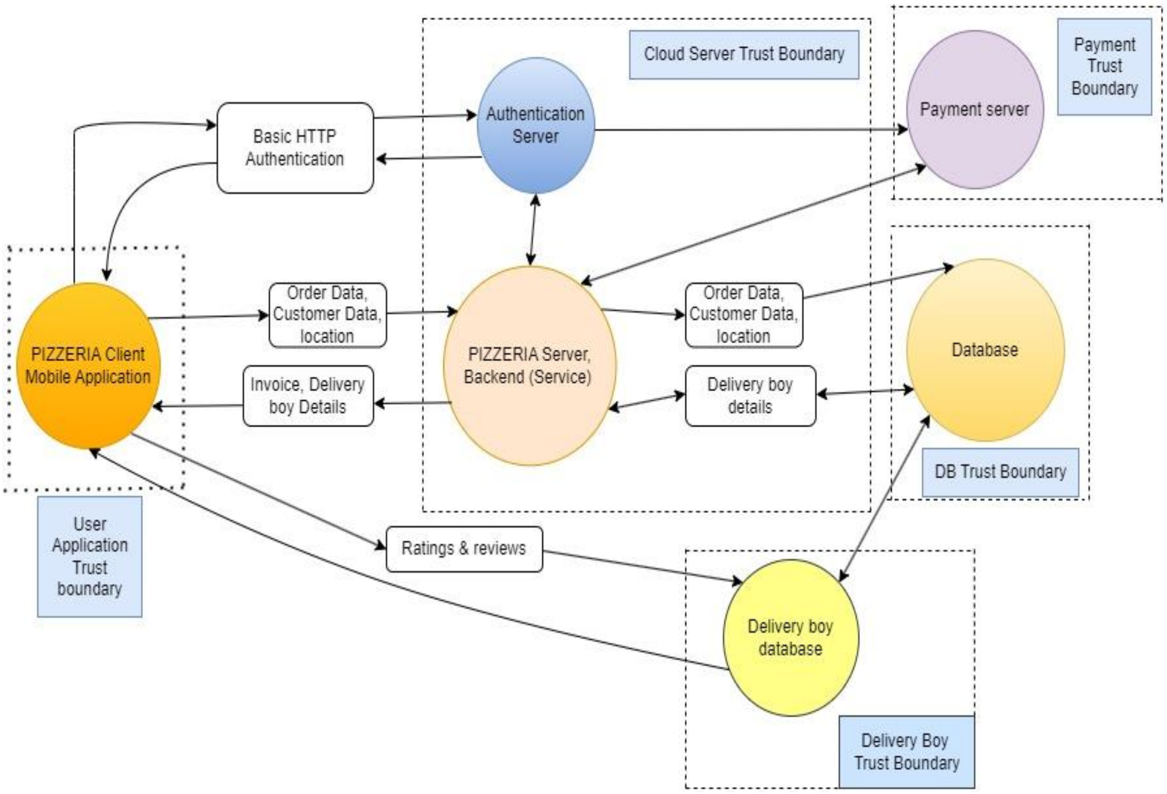
External Interfaces

- Payment Gateway
- Supplier Systems
- Customer Interaction Points:

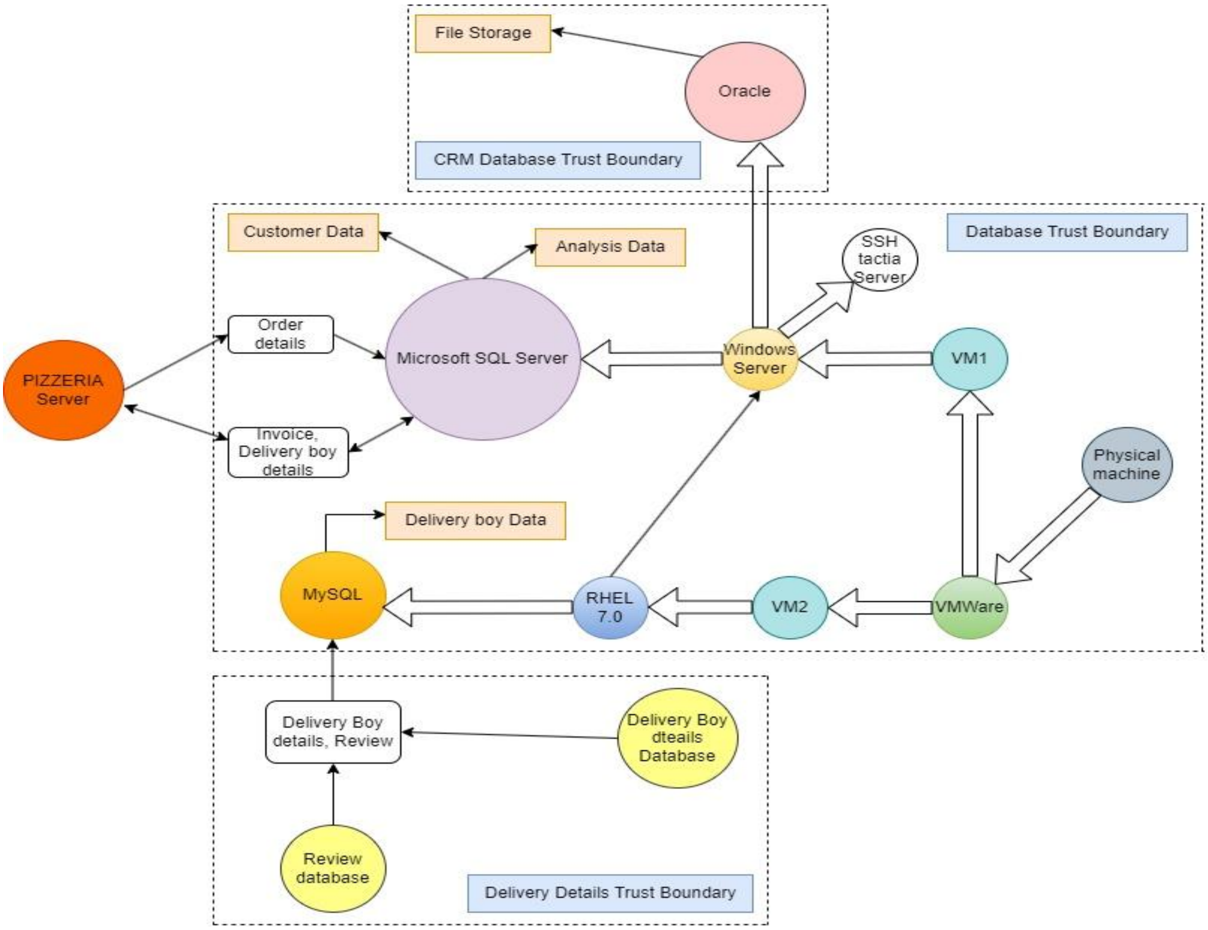
    Website: Accessible via HTTP/HTTPS for placing orders and managing customer accounts.

    Mobile App: Provides a mobile interface for customers to place orders and view promotions.

- ***App-Server DFD:***


Cloud Server Trust Boundary
Payment Trust Boundary
Basic HTTP Authentication
Authentication Server
Payment server
Order Data, Customer Data, location
PIZZERIA Client Mobile Application
PIZZERIA Server, Backend (Service)
Order Data, Customer Data, location
Database
Invoice, Delivery boy Details
Delivery boy details
DB Trust Boundary
User Application Trust boundary
Ratings & reviews
Delivery boy database
Delivery Boy Trust Boundary

- *Database DFD:*



Phase 3: Threat Analysis

For Phase 3 of a risk analysis for pizzeria, we'll identify the attacker's profile and their activities.

Step 1: Develop attacker profile

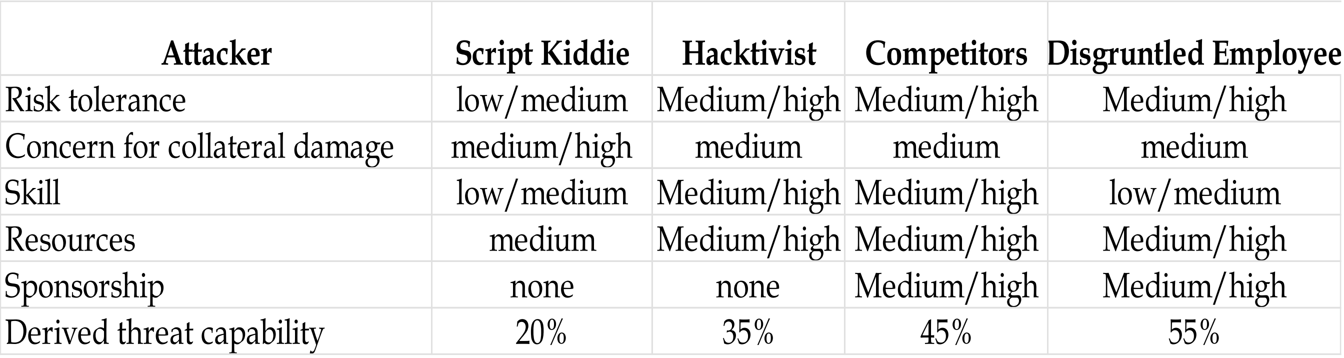
So, my first motive is to develop the attacker profile. I divided the attacker's profile in two sections as attacker attitude and attacker capabilities.

Attacker attitude is influenced by many factors. From FAIR methodology I took two conditions to evaluate attacker attitude. They are: *Risk tolerance* and *Concern for collateral damage.*

Attacker capability is simply a percentile Scale 1-100 which represents the comprehensive range of capabilities for a population of threat agents. It is mainly depending on few factors like: *Skills, Resource, Sponsorship.*

Attacker
Personal Risk tolerance
Concern for collateral damage
skill
Resources
Sponsorship
Threat capability

Now I am going to develop the attacker profile for Pizzeria:



Attacker	Script Kiddie	Hacktivist	Competitors	Disgruntled Employee
Risk tolerance	low/medium	Medium/high	Medium/high	Medium/high
Concern for collateral damage	medium/high	medium	medium	medium
Skill	low/medium	Medium/high	Medium/high	low/medium
Resources	medium	Medium/high	Medium/high	Medium/high
Sponsorship	none	none	Medium/high	Medium/high
Derived threat capability	20%	35%	45%	55%

Step 2: Develop abuse cases

Now my second motive is to develop the abuse cases.
Abuse cases are close to Loss events; loss events represent bad things that can happen and abuse cases are ways of doing these bad things.

An abuse cases is a number of attack events. It essentially specifies the start and end of the attack chains. The starting point is thought of as the attack surface, and the end is the when a successful breach is achieved that will lead to the loss event.

Abuse case has a number of properties related to our beliefs about the abuse cases being executed.

Abuse case
Accessibility to attack surfaces
Window of opportunity
Ability to repudiate
Perceived deterrence
Perceived ease of attack
Perceived benefit of success
Probability of success
Threat event probability
Probability of contact
Effort spent
Probability of action

Now I am going to develop some abuse cases for Pizzeria:

Abuse case	Render the service unavailable with a serious DDoS attack	Obtain Classified user data (using network attack)	Ordering pizza without consent	Obtain company analytics data
Number of abuse case	1	2	3	4
Target asset	Pizzeria Client (Mobile application)	User Data	Pizza	Cloud file storage
Attack surface	Pizzeria Server (backend)	Connection between client app and pizzeria server		User access to root user of Pizzeria server
Accessibility to attack surface	High	Mid	High	High
Window of opportunity	High	Mid	Low	High
Ability to repudiate	Mid/high	High	High	Low
Perceived deterrence	Mid	Mid	Mid	High
Perceived ease of attack	Low	High	Mid	Low
Perceived benefit of success	Mid	High	Mid/high	high
Threat event probability	12%	15%	1%	5%
Loss event	System Downtime	Data Loss	Order pizza without authentication, free food	Data Loss
Attacker	Competitors	Hacktivist	Script kiddie	Hacktivist
Risk tolerance (attacker)	high	Mid/high	Low/mid	high
Probability of contact	80%	50%	50%	100%

Probability of action	15%	30%	2%	5%
CIA impact breach	availability	Confidential	Integrity	Confidential

Phase 4: Attack and Resilience analysis

This phase has 2 steps:

Step 1: List of Vulnerabilities
Step 2: Design Attack Graph

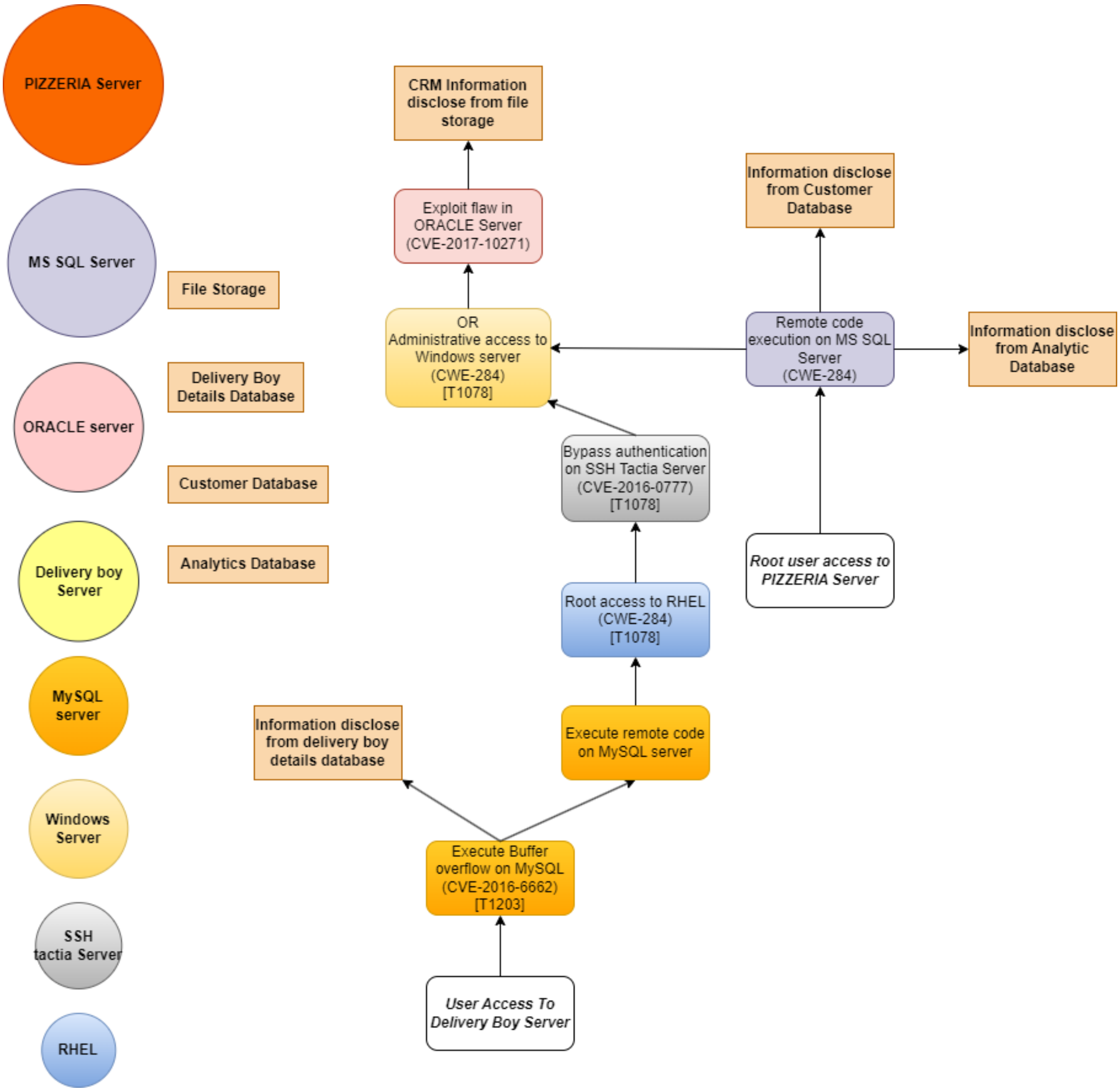
Step 1: List of vulnerabilities

Asset	Vulnerability	Description	CVE/CWE Code	MITRE Attack ID	Mitigation Techniques
Pizzeria Server	Root User Access	Unauthorized root access to the Pizzeria Server	CWE-284	T1078	Implement strong access control, regular audits
MS SQL Server	Remote Code Execution	Remote execution of arbitrary code	CVE-2016-0777	T1059	Patch the software, use IDS/IPS
Windows Server	Administrative Access	Gaining administrative access	CWE-284	T1078	Strengthen authentication mechanisms, apply patches
SSH Tactia Server	Bypass Authentication	Exploiting vulnerabilities to bypass authentication	CVE-2016-0777	T1078	Update SSH software, enforce strong authentication
RHEL	Root Access	Gaining unauthorized root access	CWE-284	T1078	Use SELinux, regular security updates

MySQL Server	Buffer Overflow	Overflowing buffers to execute arbitrary code	CVE-2016-6662	T1203	Input validation, apply patches
Delivery Boy Server	User Access	Unauthorized user access	CWE-284	T1078	Strengthen access control, regular monitoring
Delivery Boy Details Database	Information Disclosure	Leakage of sensitive delivery boy details	CWE-200	T1530	Encrypt sensitive data, implement access controls
Oracle Server	Exploit Flow	Exploiting vulnerabilities leading to further exploits	CVE-2017-10271	T1203	Regular patches, apply security best practices
File Storage	Information Disclosure	Leakage of CRM information from file storage	CWE-200	T1530	Encrypt data, enforce access control
Customer Database	Information Disclosure	Unauthorized access to customer information	CWE-200	T1530	Apply encryption, regular security audits
Analytics Database	Information Disclosure	Unauthorized access to sensitive analytical data	CWE-200	T1530	Encrypt data, enforce strong access controls

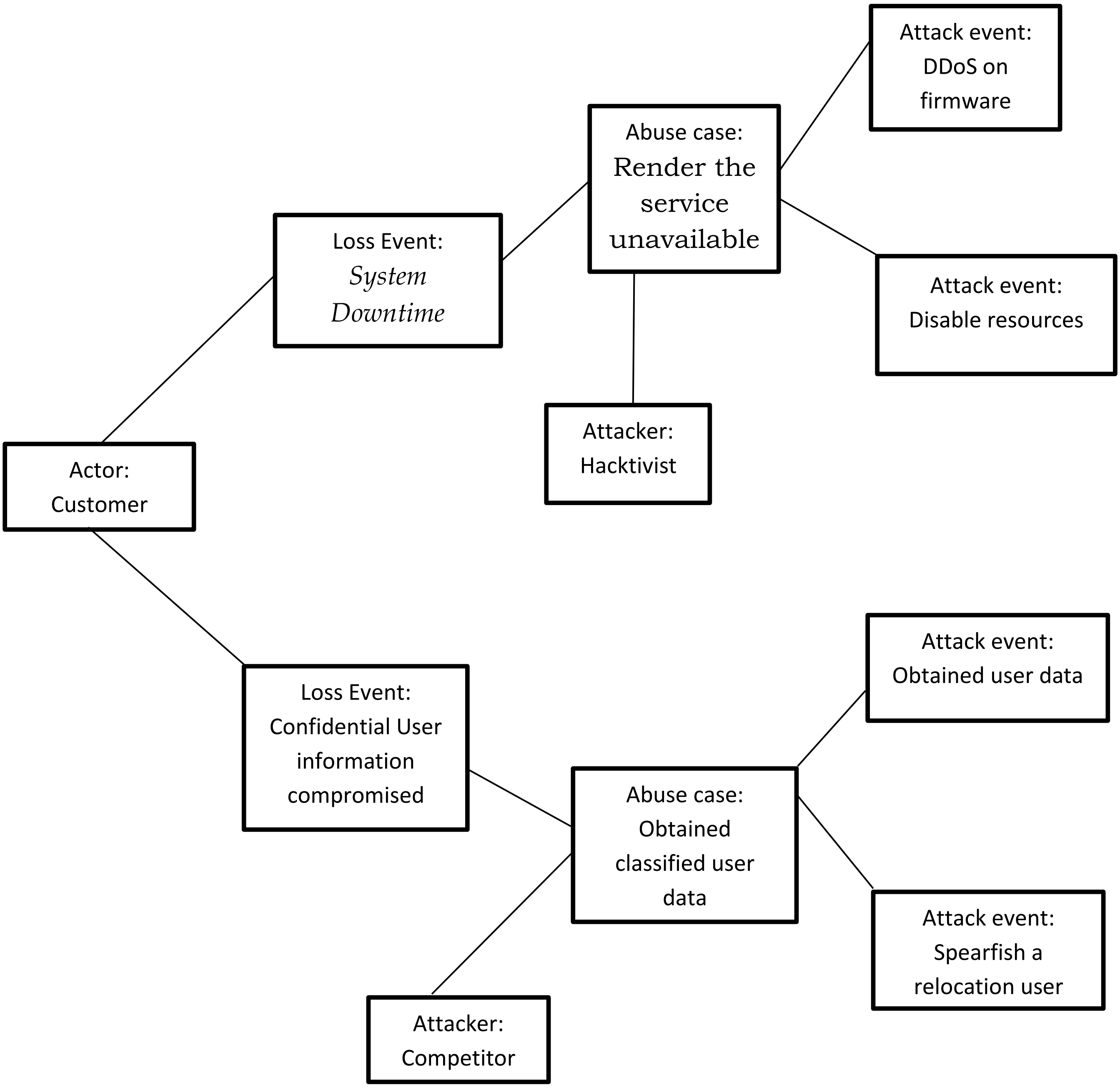
Step 2: Design Attack Graph

Obtain Company Analytics & Customer data


PIZZERIA Server
MS SQL Server
ORACLE server
Delivery boy Server
MySQL server
Windows Server
SSH tactia Server
RHEL
File Storage
Delivery Boy Details Database
Customer Database
Analytics Database
CRM Information disclose from file storage
Exploit flaw in ORACLE Server (CVE-2017-10271)
OR Administrative access to Windows server (CWE-284) [T1078]
Information disclose from Customer Database
Remote code execution on MS SQL Server (CWE-284)
Information disclose from Analytic Database
Bypass authentication on SSH Tactia Server (CVE-2016-0777) [T1078]
Root user access to PIZZERIA Server
Root access to RHEL (CWE-284) [T1078]
Information disclose from delivery boy details database
Execute remote code on MySQL server
Execute Buffer overflow on MySQL (CVE-2016-6662) [T1203]
User Access To Delivery Boy Server

Phase 5: Attack and Resilience analysis

Perform overall risk assessment



Attack event: DDoS on firmware
Abuse case: Render the service unavailable
Loss Event: *System Downtime*
Attack event: Disable resources
Attacker: Hacktivist
Actor: Customer
Attack event: Obtained user data
Loss Event: Confidential User information compromised
Abuse case: Obtained classified user data
Attack event: Spearfish a relocation user
Attacker: Competitor